Journal of Number Theory 163 (2016) 1–18

Contents lists available at ScienceDirect

Journal of Number Theory

www.elsevier.com/locate/jnt

On a divisibility relation for Lucas sequences

Yuri F. Bilu [a,1], Takao Komatsu [b,2], Florian Luca [c], Amalia Pizarro-Madariaga [d,*,3], Pantelimon Stănică [e,4]

[a] IMB, Université Bordeaux 1 & CNRS, 351 cours de la Libération, 33405 Talence, France
[b] School of Mathematics and Statistics, Wuhan University, Wuhan 430072, China
[c] School of Mathematics, University of the Witwatersrand, Private Bag X3, Wits 2050, South Africa
[d] Instituto de Matemáticas, Universidad de Valparaíso, Chile
[e] Naval Postgraduate School, Applied Mathematics Department, Monterey, CA 93943-5216, USA

ARTICLE INFO

Article history:
Received 9 October 2015
Received in revised form 24 November 2015
Accepted 26 November 2015
Available online 8 January 2016
Communicated by Steven J. Miller

MSC:
11B39

Keywords:
Lucas sequence
Roots of unity

ABSTRACT

In this note, we study the divisibility relation $U_m \mid U_{n+k}^s - U_n^s$, where $\mathbf{U} := \{U_n\}_{n \geq 0}$ is the Lucas sequence of characteristic polynomial $x^2 - ax \pm 1$ and k, m, n, s are positive integers.

* Corresponding author.
E-mail addresses: yuri@math.u-bordeaux.fr (Yu.F. Bilu), komatsu@whu.edu.cn (T. Komatsu), florian.luca@wits.ac.za (F. Luca), amalia.pizarro@uv.cl (A. Pizarro-Madariaga), pstanica@nps.edu (P. Stănică).

[1] Partially supported by the Max-Planck Institut für Mathematik.
[2] Partially supported by the Hubei provincial Expert Program in China.
[3] Partially supported by the Project DIUV-REG N° 25-2013.
[4] Also associated to the *Institute of Mathematics "Simion Stoilow" of the Romanian Academy*, Bucharest, Romania.

http://dx.doi.org/10.1016/j.jnt.2015.11.011
0022-314X/© 2016 Published by Elsevier Inc.

1. Introduction

Let $\mathbf{U} := \mathbf{U}(a, b) = \{U_n\}_{n\geq 0}$ be the Lucas sequence given by $U_0 = 0$, $U_1 = 1$ and

$$U_{n+2} = aU_{n+1} + bU_n \quad \text{for all} \quad n \geq 0, \quad \text{where} \quad b \in \{\pm 1\}. \tag{1}$$

Its characteristic equation is $x^2 - ax - b = 0$ with roots

$$(\alpha, \beta) = \left(\frac{a + \sqrt{a^2 + 4b}}{2}, \frac{a - \sqrt{a^2 + 4b}}{2} \right). \tag{2}$$

When $a \geq 1$, we have that $\alpha > 1 > |\beta|$. We assume that $\Delta = a^2 + 4b > 0$ and that α/β is not a root of unity. This only excludes the pairs $(a, b) \in \{(0, \pm 1),\ (\pm 1, -1),\ (2, -1)\}$ from the subsequent considerations. Here, we look at the relation

$$U_m \mid U_{n+k}^s - U_n^s, \tag{3}$$

with positive integers k, m, n, s. Note that when $(a, b) = (1, 1)$, then $U_n = F_n$ is the nth Fibonacci number. Taking $k = 1$ and using the relations

$$\begin{aligned} F_{n+1} - F_n &= F_{n-1}, \\ F_{n+1} + F_n &= F_{n+2}, \\ F_{n+1}^2 + F_n^2 &= F_{2n+1}, \end{aligned}$$

it follows that relation (3) holds with $s = 1, 2, 4$, and $m = n-1,\ n+1,\ 2n+1$, respectively. Further, in [2], the authors assumed that m and n are coprime positive integers. In this case, F_n and F_m are coprime, so the rational number F_{n+1}/F_n is defined modulo F_m. Then it was shown in [2] that if this last congruence class above has multiplicative order s modulo F_m and $s \notin \{1, 2, 4\}$, then

$$m < 500s^2. \tag{4}$$

In this paper, we study the general divisibility relation (3) and prove the following result.

Theorem 1. *Let a be a non-zero integer, $b \in \{\pm 1\}$, and k a positive integer. Assume that $(a, b) \notin \{(\pm 1, -1),\ (\pm 2, -1)\}$. Given a positive integer m, let s be the smallest positive integer such that divisibility (3) holds. Then either $s \in \{1, 2, 4\}$, or*

$$m < 20000(sk)^2. \tag{5}$$

2. Preliminary results

We put $\mathbf{V} := \mathbf{V}(a,b) = \{V_n\}_{n\geq 0}$ for the Lucas companion of $\mathbf{U}$ which has initial values $V_0 = 2$, $V_1 = a$ and satisfies the same recurrence relation $V_{n+2} = aV_{n+1} + bV_n$ for all $n \geq 0$. The Binet formulas for U_n and V_n are

$$U_n = \frac{\alpha^n - \beta^n}{\alpha - \beta}, \qquad V_n = \alpha^n + \beta^n \qquad \text{for all} \qquad n \geq 0. \tag{6}$$

The next result addresses the period of $\{U_n\}_{n\geq 0}$ modulo U_m, where $m \geq 1$ is fixed.

Lemma 2. *The congruence*

$$U_{n+4m} \equiv U_n \pmod{U_m} \tag{7}$$

holds for all $n \geq 0$, $m \geq 2$.

Proof. This follows because of the identity

$$U_{n+4m} - U_n = U_m V_m V_{n+2m},$$

which can be easily checked using the Binet formulas (6). □

The following is Lemma 1 in [2]. It has also appeared in other places.

Lemma 3. *Let $X \geq 3$ be a real number. Let a and b be positive integers with $\max\{a,b\} \leq X$. Then there exist integers u, v not both zero with $\max\{|u|,|v|\} \leq \sqrt{X}$ such that $|au + bv| \leq 3\sqrt{X}$.*

The following lemma is well-known, but we include the proof for the reader's convenience. In what follows, a unit means Dirichlet unit, that is an algebraic integer η such that η^{-1} is also an algebraic integer.

Lemma 4. *Let $v > 1$ be an integer and ζ be a primitive vth root of unity. Then*

$$\prod_{\gcd(k,v)=1} (1 - \zeta^k) = \begin{cases} p, & \text{if } v = p^\ell \text{ is a prime power,} \\ 1, & \text{if } v \text{ has at least two distinct prime divisors,} \end{cases} \tag{8}$$

the product being over the residue classes $\bmod\ v$ coprime with v. In particular, in the second case, $1 - \zeta$ is a unit.

Proof. The product on the left of (8) is $\Phi_v(1)$, where $\Phi_v(X)$ denotes the vth cyclotomic polynomial. For $v = p^\ell$ we have

$$\Phi_{p^\ell}(X) = \frac{X^{p^\ell} - 1}{X^{p^{\ell-1}} - 1} = X^{p^{\ell-1}(p-2)} + X^{p^{\ell-1}(p-1)} + \cdots + X^{p^{\ell-1}} + 1,$$

and $\Phi_{p^\ell}(1) = p$, proving the prime power case. In particular, $(1-\zeta) \mid p$ in this case.

Now assume that v is divisible by two distinct primes p and p'. Then $\zeta^{v/p}$ is a primitive root of unity of order p, which implies that in the ring $\mathbb{Z}[\zeta]$ we have $(1-\zeta) \mid (1-\zeta^{v/p}) \mid p$. Similarly, $(1-\zeta) \mid p'$. The divisibility relations $(1-\zeta) \mid p$ and $(1-\zeta) \mid p'$ imply that $(1-\zeta) \mid 1$, that is, $1-\zeta$ is a unit. Hence its $\mathbb{Q}(\zeta)/\mathbb{Q}$-norm is ± 1. Since it is obviously positive, it must be 1. But this norm is exactly the left-hand side of (8). □

This lemma has the following consequence, which is again well-known, but we did not find a suitable reference.

Corollary 5.

1. *Assume that ζ and ξ are roots of unity of coprime orders, and both distinct from* 1. *The $\zeta - \xi$ is a unit.*
   From now on m and n are positive integers and $d = \gcd(m, n)$.
2. *In $\mathbb{Z}[x]$ we have the equality of ideals $(x^m - 1, x^n - 1) = (x^d - 1)$.*
3. *Let γ be an algebraic integer in some number field K. Then we have the equality of $\mathcal{O}_K$-ideals $(\gamma^m - 1, \gamma^n - 1) = (\gamma^d - 1)$.*

Proof. Item 1 follows from the second assertion of Lemma 4.

In item 2 it suffices to show that $x^d - 1 \in (x^m - 1, x^n - 1)$. In the case $d = 1$ this reduces to showing that

$$1 \in \left(\frac{x^m - 1}{x - 1}, \frac{x^n - 1}{x - 1} \right). \tag{9}$$

The resultant of the polynomials $\frac{x^m-1}{x-1}$ and $\frac{x^n-1}{x-1}$ is the product of the factors of the form $\zeta - \xi$, where ζ and ξ are roots of unity of orders dividing m and n, respectively, and none of ζ, ξ is 1. If $d = \gcd(m, n) = 1$, then each factor is a unit by item 1. Hence, the resultant is a unit of $\mathbb{Z}$, that is, ± 1, proving (9) in the case $d = 1$.

The case of arbitrary d reduces to the case $d = 1$. Indeed, by the latter, $x^d - 1$ belongs to the ideal $(x^m - 1, x^n - 1)$ in the ring $\mathbb{Z}[x^d]$. Hence, the same is true in the ring $\mathbb{Z}[x]$.

Finally, item 3 is an immediate consequence of the previous item. □

We will use one simple property of cyclotomic polynomials. Recall that for a positive integer v we denote by $\Phi_v(X)$ the vth cyclotomic polynomial. Then for $\alpha > 1$ we have the trivial estimate $\Phi_v(\alpha) > (\alpha - 1)^{\varphi(v)}$ (where $\varphi(v)$ is, of course, the Euler totient). We will need a slightly sharper estimate.

Lemma 6. *Let v be a positive integer and $\alpha > 1$ a real number. Then for $v > 1$ we have*

$$\Phi_v(\alpha) > \big(\alpha(\alpha-1)\big)^{\varphi(v)/2}. \tag{10}$$

Proof. We use the identity

$$\Phi_v(X) = \prod_{d\mid v}(X^d-1)^{\mu(v/d)},$$

where $\mu(\cdot)$ is the Möbius function. We have clearly

$$(\alpha^d-1)^{\mu(v/d)} \ge \begin{cases}\alpha^{d\mu(v/d)}, & \mu(v/d)=-1,\\ \alpha^{d\mu(v/d)}\frac{\alpha-1}{\alpha}, & \mu(v/d)=1.\end{cases} \tag{11}$$

Moreover:

- denoting by $\tau^*(v)$ the number of square-free divisors of v, we have, for $v > 1$, exactly $\tau^*(v)/2$ divisors with $\mu(v/d) = 1$ and exactly $\tau^*(v)/2$ divisors with $\mu(v/d) = -1$;
- inequality (11) is strict for all $d \mid v$ satisfying $\mu(v/d) \neq 0$, with at most one exception.

Hence, multiplying (11) for all $d \mid v$ with $\mu(v/d) \neq 0$, and using the identity $\varphi(v) = \sum_{d\mid v} d\mu(v/d)$, we obtain, for $v > 1$, the lower estimate

$$\Phi_v(\alpha) > \alpha^{\varphi(v)}\left(\frac{\alpha-1}{\alpha}\right)^{\tau^*(v)/2}. \tag{12}$$

For $v \notin \{1,2,6\}$, we have $\tau^*(v) \le \varphi(v)$, which implies

$$|\Phi_v(\alpha)| > \alpha^{\varphi(v)}\left(\frac{\alpha-1}{\alpha}\right)^{\varphi(v)/2} = \big(\alpha(\alpha-1)\big)^{\varphi(v)/2},$$

proving (10) for $v \notin \{1,2,6\}$. And for $v \in \{2,6\}$, this is obviously true. □

The following lemma is the workhorse of our argument.

Lemma 7. *Let a, b and k be as in the statement of Theorem 1, and assume in addition that $a \ge 1$. Let $v \ge 1$ be an integer and ζ a primitive vth root of unity. Define α as in (2) and assume that the numbers*

$$\alpha \qquad \text{and} \qquad \frac{\alpha^k-(-b)^k\bar{\zeta}}{\alpha^k-\zeta} \tag{13}$$

are multiplicatively dependent. Then we have one of the following options:

(*i*) $(-b)^k = -1$, $v = 4$;
(*ii*) $(a, b, k) \in \{(1, 1, 1),\ (2, 1, 1)\}$ *and* $v \in \{1, 2\}$;
(*iii*) $(-b)^k = 1$, $v \in \{1, 2\}$;
(*iv*) $(a, b, k) = (4, -1, 1)$ *and* $v \in \{4, 6\}$.

Proof. We use the notation

$$K = \mathbb{Q}(\alpha), \quad L = \mathbb{Q}(\zeta), \quad M = \mathbb{Q}(\alpha, \zeta), \quad \alpha_1 = \alpha^k, \quad \delta = (-b)^k.$$

Note that $\delta\alpha_1^{-1} = \beta^k$ is the Galois conjugate of α_1.

Recall that we disregard the cases $(a, b) \in \{(1, -1), (2, -1)\}$. In addition to this, we will disregard the case $(a, b, k) = (1, 1, 1)$, because it is settled in Lemma 2 of [2]. This implies that

$$\alpha_1 \geq 1 + \sqrt{2}. \tag{14}$$

When $\delta = 1$ we can say more:

$$\alpha_1 \in \left\{\frac{3+\sqrt{5}}{2}, 2+\sqrt{3}\right\} \quad \text{or} \quad \alpha_1 \geq \frac{5+\sqrt{21}}{2}. \tag{15}$$

We will also assume that we are not in one of the instances (*i*), (*iii*) above; this is equivalent to saying that

$$\zeta^2 \neq \delta. \tag{16}$$

Since the numbers (13) are multiplicatively dependent, then the second of these numbers must be a unit (because the first is). In particular,

$$(\alpha_1 - \zeta) \mid (\alpha_1 - \delta\bar{\zeta})$$

in the ring $\mathcal{O}_M$, which implies that

$$(\alpha_1 - \zeta) \mid (\zeta - \delta\bar{\zeta}). \tag{17}$$

This divisibility relation is very restrictive: we will see that is satisfied in very few cases, which can be verified by inspection.

We first show the following identity for the norm of $\alpha_1 - \zeta$:

$$|\mathcal{N}_{M/\mathbb{Q}}(\alpha_1 - \zeta)| = \left(\alpha_1^{-\varphi(v)}\Phi_v(\alpha_1)\Phi_{v^*}(\alpha_1)\right)^{[M:L]/2}, \tag{18}$$

where $\Phi_v(X)$ is the vth cyclotomic polynomial and

$$v^* = \begin{cases} v & \text{if } 4 \mid v \text{ or } \delta = 1, \\ v/2 & \text{if } 2 \parallel v \text{ and } \delta = -1, \\ 2v & \text{if } 2 \nmid v \text{ and } \delta = -1. \end{cases} \tag{19}$$

Note that

$$\varphi(v^*) = \varphi(v), \qquad \Phi_{v^*}(X) = \pm\Phi_v(\delta X), \qquad \Phi_v(X^{-1}) = \pm X^{-\varphi(v)}\Phi_v(X),$$

the sign in last identity being "+" for $v > 1$ and the sign in the middle identity being "+" if $\delta = 1$ or $\min\{v, v^*\} > 1$.

Let us prove (18). When $\alpha \notin L$, the conjugates of $\alpha_1 - \zeta$ are the $2\varphi(v)$ numbers $\alpha_1 - \zeta'$ and $\delta\alpha_1^{-1} - \zeta''$, where both ζ' and ζ'' run through the set of primitive vth roots of unity. Hence, in this case

$$|\mathcal{N}_{M/\mathbb{Q}}(\alpha_1 - \zeta)| = |\Phi_v(\alpha_1)\Phi_v(\delta\alpha_1^{-1})| = \alpha_1^{-\varphi(v)}\Phi_v(\alpha_1)\Phi_{v^*}(\alpha_1),$$

which is (18) in the case $\alpha \notin L$.

Now assume that $\alpha \in L$, and set

$$G = \mathrm{Gal}(L/\mathbb{Q}), \qquad H = \mathrm{Gal}(L/K),$$

for the Galois groups of the various extensions. The group H is a subgroup of G of index 2, and we have

$$\alpha_1^\sigma = \begin{cases} \alpha_1, & \sigma \in H, \\ \delta\alpha_1^{-1}, & \sigma \in G \smallsetminus H. \end{cases}$$

Hence,

$$\begin{aligned} |\mathcal{N}_{M/\mathbb{Q}}(\alpha_1 - \zeta)| &= |\mathcal{N}_{L/\mathbb{Q}}(\alpha_1 - \zeta)| \\ &= \prod_{\sigma\in H} |\alpha_1 - \zeta^\sigma| \prod_{\sigma\in G\smallsetminus H} |\delta\alpha_1^{-1} - \zeta^\sigma| \\ &= \alpha_1^{-\varphi(v)/2} \prod_{\sigma\in H} |\alpha_1 - \zeta^\sigma| \prod_{\sigma\in G\smallsetminus H} |\delta\alpha_1 - \zeta^\sigma|, \end{aligned}$$

where in the second equality we used $\alpha_1 \in \mathbb{R}$. In a similar fashion,

$$\begin{aligned} |\mathcal{N}_{M/\mathbb{Q}}(\alpha_1 - \delta\bar{\zeta})| &= \prod_{\sigma\in H} |\alpha_1 - \delta\bar{\zeta}^\sigma| \prod_{\sigma'\in G\smallsetminus H} |\delta\alpha_1^{-1} - \delta\bar{\zeta}^\sigma| \\ &= \alpha_1^{-\varphi(v)/2} \prod_{\sigma\in H} |\delta\alpha_1 - \zeta^\sigma| \prod_{\sigma\in G\smallsetminus H} |\alpha_1 - \zeta^\sigma|. \end{aligned}$$

Since $\frac{\alpha_1 - \delta\bar{\zeta}}{\alpha_1 - \zeta}$ is a unit, the two norms computed above are equal. Hence,

$$\begin{aligned}|\mathcal{N}_{M/\mathbb{Q}}(\alpha_1-\zeta)|^2 &= |\mathcal{N}_{M/\mathbb{Q}}(\alpha_1-\zeta)\mathcal{N}_{M/\mathbb{Q}}(\alpha_1-\delta\bar{\zeta})| \\ &= \alpha_1^{-\varphi(v)}\prod_{\sigma\in G}|\alpha_1-\zeta^\sigma|\prod_{\sigma\in G}|\delta\alpha_1-\zeta^\sigma| \\ &= \alpha_1^{-\varphi(v)}\Phi_v(\alpha_1)\Phi_{v^*}(\alpha_1),\end{aligned}$$

which proves (18) in the case $\alpha \in L$ as well.

Combining (17) and (18) and recalling (16), we obtain the inequality

$$0 < \alpha_1^{-\varphi(v)/2}|\Phi_v(\alpha_1)\Phi_{v^*}(\alpha_1)|^{1/2} \le |\mathcal{N}_{L/\mathbb{Q}}(1-\delta\zeta^2)|. \tag{20}$$

This will be our basic tool.

Our next observation is that $1-\delta\zeta^2$ cannot be a unit. Indeed, if it is a unit, then the right-hand side of (20) is 1 and $\min\{v, v^*\} > 1$. Hence, applying Lemma 6, we obtain

$$\alpha_1^{-\varphi(v)/2}\big(\alpha_1(\alpha_1-1)\big)^{\varphi(v)/2} < 1,$$

which implies $\alpha_1 < 2$, contradicting (14).

Thus, $1-\delta\zeta^2$ is non-zero, but not a unit. Applying Lemma 4, we find that this is possible only in the following cases:

$$v = p^\ell, \qquad \delta = 1, \tag{21}$$

$$v = 2p^\ell, \qquad \delta = 1, \tag{22}$$

$$v = 2^\ell, \qquad \ell \ge 3, \tag{23}$$

$$v \in \{1, 2, 4\}, \qquad \delta \ne \zeta^2, \tag{24}$$

where (here and below) ℓ is a positive integer and p is an odd prime number. We study these cases separately.

In the case (21), we have

$$\Phi_v(X) = \Phi_{v^*}(X) = \frac{X^{p^\ell}-1}{X^{p^{\ell-1}}-1} \qquad \text{and} \qquad \mathcal{N}_{L/\mathbb{Q}}(1-\zeta^2) = p$$

by Lemma 4. We obtain

$$\frac{1}{\alpha_1^{p^{\ell-1}(p-1)/2}}\frac{\alpha_1^{p^\ell}-1}{\alpha_1^{p^{\ell-1}}-1} \le p.$$

The left-hand side is strictly bounded from below by $\alpha^{p^{\ell-1}(p-1)/2}$, which gives $\alpha_1^{p^{\ell-1}} < p^{\frac{2}{p-1}}$. Checking with (15) leaves the only option

$$\alpha_1 = \frac{3+\sqrt{5}}{2}, \qquad p^\ell = 3,$$

which is eliminated by direct verification.

In the case (22), we have

$$\Phi_v(X) = \Phi_{v^*}(X) = \frac{X^{p^\ell}+1}{X^{p^{\ell-1}}+1} \qquad \text{and} \qquad \mathcal{N}_{L/\mathbb{Q}}(1-\zeta^2) = p.$$

We obtain

$$\frac{1}{\alpha_1^{p^{\ell-1}(p-1)/2}} \frac{\alpha_1^{p^\ell}+1}{\alpha_1^{p^{\ell-1}}+1} \le p.$$

From (15), we deduce $\alpha_1^{p^{\ell-1}}+1 \le 1.4\,\alpha_1^{p^{\ell-1}}$, which implies the inequality $\alpha_1^{p^{\ell-1}} < (1.4\,p)^{\frac{2}{p-1}}$. Invoking again (15), we are left with the three options

$$\alpha_1 = \frac{3+\sqrt{5}}{2}, \qquad p^\ell \in \{3,5\}, \tag{25}$$

$$\alpha_1 = 2+\sqrt{3}, \qquad p^\ell = 3. \tag{26}$$

The two cases in (25) are eliminated by verification, while (26) leads to $(a,b,k,v) = (4,-1,1,6)$, one of the two instances in (*iv*).

In the case (23), we have

$$\Phi_v(X) = \Phi_{v^*}(X) = \frac{X^{2^\ell}-1}{X^{2^{\ell-1}}-1} \qquad \text{and} \qquad \mathcal{N}_{L/\mathbb{Q}}(1-\delta\zeta^2) = 4.$$

We obtain

$$\frac{1}{\alpha_1^{2^{\ell-2}}} \frac{\alpha_1^{2^\ell}-1}{\alpha_1^{2^{\ell-1}}+1} \le 4,$$

which implies $\alpha_1^{2^{\ell-2}} \le 4$. Since $\ell \ge 3$, this contradicts (14).

In the final case (24), it more convenient to use the divisibility relation (17) directly. If $v \in \{1,2\}$, then $\zeta^2 = 1$ and $\delta = -1$. Taking the norm in both sides of (17), we obtain

$$\alpha_1 - \alpha_1^{-1} = \mathrm{Tr}_{K/\mathbb{Q}}(\alpha_1) \mid 4.$$

Together with $\mathcal{N}_{K/\mathbb{Q}}(\alpha_1) = \delta = -1$ and inequality (14), this implies two possibilities:

$$\alpha_1 = 1+\sqrt{2}, \quad \alpha_1 = 2+\sqrt{3}. \tag{27}$$

The latter is disqualified by inspection. The former yields $(a,b,k) = (2,1,1)$, which is (*ii*).

In a similar fashion one treats $v = 4$. In this case $\zeta^2 = -1$ and $\delta = 1$, and, taking the norm in (17), we obtain

$$(\alpha_1 + \alpha_1^{-1})^2 = (\mathrm{Tr}_{K/\mathbb{Q}}(\alpha_1))^2 \mid 16.$$

We again have one of the options (27), but this time the former is eliminated by inspection, and the latter leads to $(a, b, k) = (4, -1, 1)$, the missing instance in (iv). This completes the proof of the lemma. □

The following is a generalization of Lemma 4 from [2].

For a prime number p and a nonzero integer m, we put $\nu_p(m)$ for the exponent of the prime p in the factorization of m. For a finite set of primes $\mathcal{S}$ and a positive integer m, we put

$$m_{\mathcal{S}} = \prod_{p\in\mathcal{S}} p^{\nu_p(m)}$$

for the largest divisor of m whose prime factors are in $\mathcal{S}$. For any prime number p we put f_p for the index of appearance in the Lucas sequence $\{U_n\}_{n\geq 0}$, which is the minimal positive integer k such that $p \mid U_k$.

Lemma 8. *Let $a \geq 1$. If $\mathcal{S}$ is any finite set of primes and m is a positive integer, then*

$$(U_m)_{\mathcal{S}} \leq \alpha^2 m \operatorname{lcm}[U_{f_p} : p \in \mathcal{S}].$$

Proof. It is known that

$$\nu_p(U_m) = \begin{cases} 0 & \text{if} \quad m \not\equiv 0 \pmod{f_p}; \\ \nu_p(U_{f_p}) + \nu_p(m/f_p) & \text{if} \quad m \equiv 0 \pmod{f_p}, \qquad p \text{ odd}; \\ \nu_2(U_2) + \nu_2(m/2) & \text{if} \quad m \equiv 0 \pmod{2}, \quad p = 2,\ a \text{ even}; \\ \nu_2(U_3) & \text{if} \quad m \equiv 3 \pmod{6}, \quad p = 2,\ a \text{ odd}; \\ \nu_2(U_6) + \nu_2(m/2) & \text{if} \quad m \equiv 0 \pmod{6}, \quad p = 2,\ a \text{ odd}. \end{cases}$$

The above relations follow easily from Proposition 2.1 in [1]. In particular, the inequality

$$\nu_p(U_m) \leq \nu_p(U_{f_p}) + \nu_p(m) + \delta_{p,2}$$

always holds with $\delta_{p,2}$ being 0 if p is odd or $p = 2$ and a is even and $\nu_2((a^2 + 3b)/2)$ if $p = 2$ and a is odd. We get that

$$\begin{aligned} (U_m)_{\mathcal{S}} &\leq \left(\prod_{p\in\mathcal{S}} p^{\nu_p(U_{f_p})}\right)\left(\prod_{\substack{p\mid m\\ p>2}} p^{\nu_p(m)}\right) 2^{\nu_2(m)+\nu_2((a^2+3b)/2)} \\ &< \alpha^2 m \operatorname{lcm}[U_{f_p} : p \in \mathcal{S}], \end{aligned}$$

which is what we wanted to prove. For the last inequality above, we used the fact that $2^{\nu_2((a^2+3b)/2)} \leq (a^2 + 3b)/2 = (\alpha^2 - \alpha\beta + \beta^2)/2 < \alpha^2$. □

3. Proof of Theorem 1

We assume that $m \geq 10000k$. Since U_n is periodic modulo U_m with period $4m$ (Lemma 2), we may assume that $n \leq 4m$. We split U_m into various factors, as follows. Write

$$U_{n+k}^s - U_n^s = \prod_{d|s} \Phi_d(U_{n+k}, U_n),$$

where $\Phi_d(X, Y)$ is the homogenization of the cyclotomic polynomial $\Phi_d(X)$. We put $s_1 := \mathrm{lcm}[2, s]$, $\mathcal{S} := \{p : p \mid 6s\}$ and

$$\begin{aligned}
D &:= (U_m)_{\mathcal{S}};\\
A &:= \gcd(U_m/D, \prod_{d\leq 6,\ d\neq 5} \Phi_d(U_{n+k}, U_n);\\
E &:= \gcd(U_m/D, \prod_{\substack{d|s_1\\ d=5 \text{ or } d>6}} \Phi_d(U_{n+k}, U_n).
\end{aligned}$$

Clearly,

$$U_m \mid ADE.$$

Before bounding A, D, E, let us comment on the sign of a. If $a < 0$, then we change the pair (a, b) to $(-a, b)$. This has as effect replacing (α, β) by $(-\alpha, -\beta)$ and so $U_n(\alpha, \beta) = (-1)^{n-1}U_n(\alpha, \beta)$ for all $n \geq 0$. In particular, U_m remains the same or changes sign. Further, if k is even then

$$\Phi_d(U_{n+k}(-\alpha, -\beta), U_n(-\alpha, -\beta)) = \pm\Phi_d(U_{n+k}(\alpha, \beta), U_n(\alpha, \beta)),$$

while if k is odd, then

$$\begin{aligned}
\Phi_d(U_{n+k}(-\alpha, -\beta), U_n(-\alpha, -\beta)) &= \pm\Phi_d(U_{n+k}(\alpha, \beta), -U_n(\alpha, \beta))\\
&= \pm\Phi_{d^*}(U_{n+k}(\alpha, \beta), U_n(\alpha, \beta)),
\end{aligned}$$

where the d^* has been defined at (19). Note that the sets $\{d \leq 6,\ d \neq 5\}$ and $\{d \mid s_1,$ $d = 5$ or $d > 6\}$ are closed under the operation $d \mapsto d^*$. Hence, D, A, E do not change if we replace a by $-a$, so we assume that $a > 0$. By the Binet formula (6), we get easily that the inequality

$$\alpha^{n-2} \leq U_n \leq \alpha^n \quad \text{is valid for all} \quad n \geq 1. \tag{28}$$

We are now ready to bound A, D, E.

The easiest to bound is D. Namely, by Lemma 8 and the fact that $f_p \le p+1$ for all $p \mid 6s$, we get

$$D \le \alpha^2 m \prod_{p \mid 6s} U_{p+1} < m\alpha^{2+\sum_{p\mid 6s}(p+1)} < \alpha^{6s+3+\log m/\log\alpha}, \tag{29}$$

where we used the fact that $\sum_{p\mid t}(p+1) \le t+1$, which is easily proved by induction on the number of distinct prime factors of t.

We next bound E.

Note that

$$E \mid \prod_{\substack{\zeta:\zeta^{s_1}=1\\ \zeta\notin\{\pm1,\pm i,\pm\omega,\pm\omega^2\}}} (U_{n+k} - \zeta U_n), \tag{30}$$

where $\omega := e^{2\pi i/3}$ is a primitive root of unity of order 3.

Let $K = \mathbb{Q}(e^{2\pi i/s_1}, \alpha)$, which is a number field of degree $d \le 2\phi(s_1) = 2\phi(s)$. Assume that there are ℓ roots of unity ζ participating in the product appearing in the right-hand side of (30) and label them $\zeta_1, \ldots, \zeta_\ell$. Write

$$\mathcal{E}_i = \gcd(E, U_{n+k} - \zeta_i U_n) \quad \text{for all} \quad i = 1, \ldots, \ell, \tag{31}$$

where $\mathcal{E}_i$ are ideals in $\mathcal{O}_K$. Then relations (30) and (31) tell us that

$$E\mathcal{O}_K \mid \prod_{i=1}^{\ell} \mathcal{E}_i. \tag{32}$$

Our next goal is to bound the norm $|\mathcal{N}_{K/\mathbb{Q}}(\mathcal{E}_i)|$ of $\mathcal{E}_i$ for $i = 1, \ldots, \ell$. First of all, $U_m \in \mathcal{E}_i$. Thus, with formula (6) and the fact that $\beta = (-b)\alpha^{-1}$, we get

$$\alpha^m \equiv (-b)^m \alpha^{-m} \pmod{\mathcal{E}_i}.$$

Multiplying the above congruence by α^m, we get

$$\alpha^{2m} \equiv (-b)^m \pmod{\mathcal{E}_i}. \tag{33}$$

We next use formulae (6) and (31) to deduce that

$$(\alpha^{n+k} - (-b)^{n+k}\alpha^{-n-k}) - \zeta(\alpha^n - (-b)^n\alpha^{-n}) \equiv 0 \pmod{\mathcal{E}_i}, \quad (\zeta := \zeta_i).$$

Multiplying both sides above by α^n, we get

$$\alpha^{2n}(\alpha^k - \zeta) - (-b)^{n+k}(\alpha^{-k} - (-b)^k\zeta) \equiv 0 \pmod{\mathcal{E}_i}. \tag{34}$$

Let us show that $\alpha^k - \zeta$ and $\mathcal{E}_i$ are coprime. Assume this is not so and let π be some prime ideal of $\mathcal{O}_{\mathbb{K}}$ dividing both $\alpha^k - \zeta$ and $\mathcal{E}_i$. Then we get $\alpha^k \equiv \zeta \pmod{\pi}$ and so $\alpha^{-k} \equiv (-b)^k \zeta \pmod{\pi}$ by (34). Multiplying these two congruences we get $1 \equiv (-b)^k \zeta^2 \pmod{\pi}$. Hence, $\pi \mid 1 - (-b)^k \zeta^2$. If this number is not zero, then, $(-b)^k \zeta^2$ is a root of unity whose order divides $6s$, so, by Lemma 6, we get that $\pi \mid 6s$, which is impossible because $\pi \mid \mathcal{E}_i \mid E$, and E is an integer coprime to $6s$. If the above number is zero, we get that $\zeta^2 = \pm 1$, so $\zeta \in \{\pm 1, \pm i\}$, but these values are excluded at this step. Thus, indeed $\alpha^k - \zeta$ and $\mathcal{E}_i$ are coprime, so $\alpha^k - \zeta$ is invertible modulo $\mathcal{E}_i$. Now congruence (34) shows that

$$\alpha^{2n+k} \equiv (-b)^n \zeta \left(\frac{\alpha^k - (-b)^k \overline{\zeta}}{\alpha^k - \zeta} \right) \pmod{\mathcal{E}_i}. \tag{35}$$

We now apply Lemma 3 to $a = 2m$ and $b = 2n + k \leq 8m + k < 9m$ with the choice $X = 9m$ to deduce that there exist integers u, v not both zero with $\max\{|u|, |v|\} \leq \sqrt{X}$ such that $|2mu + (2n + k)v| \leq 3\sqrt{X}$. We raise congruence (33) to u and congruence (35) to v and multiply the resulting congruences getting

$$\alpha^{2mu+(2n+k)v} = (-b)^{mu+nv} \zeta^v \left(\frac{\alpha^k - (-b)^k \overline{\zeta}}{\alpha^k - \zeta} \right)^v \pmod{\mathcal{E}_i}.$$

We record this as

$$\alpha^R \equiv \eta \left(\frac{\alpha^k - (-b)^k \overline{\zeta}}{\alpha^k - \zeta} \right)^S \pmod{\mathcal{E}_i} \tag{36}$$

for suitable roots of unity η and ζ of order dividing s_1 with ζ not of order $1, 2, 3, 4$, or 6, where $R := 2mu + (2n + k)v$ and $S := v$. We may assume that $R \geq 0$, for if not, we replace the pair (u, v) by the pair $(-u, -v)$, thus replacing (R, S) by $(-R, -S)$ and η by η^{-1} and leaving ζ unaffected. We may additionally assume that $S \geq 0$, for if not, we replace S by $-S$ and ζ by $(-b)^k \overline{\zeta}$, again a root of unity of order dividing s_1 but not of order $1, 2, 3, 4$, or 6 and leave R and η unaffected. Thus, $\mathcal{E}_i$ divides the algebraic integer

$$E_i = \alpha^R (\alpha^k - \zeta_i)^S - \eta_i (\alpha^k - (-b)^k \overline{\zeta_i})^S. \tag{37}$$

Let us show that $E_i \neq 0$. If $E_i = 0$, we then get

$$\alpha^R = \eta_i \left(\frac{\alpha - (-b)^k \overline{\zeta_i}}{\alpha - \zeta_i} \right)^S,$$

and after raising both sides of the above equality to the power s_1, we get, since $\eta_i^{s_1} = 1$, that

$$\alpha^{s_1 R} = \left(\frac{\alpha^k - (-b)^k \overline{\zeta_i}}{\alpha - \zeta_i} \right)^{S s_1}.$$

Lemma 7 gives us a certain number of conditions all of which have ζ_i or a root of unity of order $1, 2, 4$, or 6, which is not our case. Thus, E_i is not equal to zero. We now bound the absolute values of the conjugates of E_i. We find it more convenient to work with the associate of E_i given by

$$G_i = \alpha^{-\lfloor R/2\rfloor} E_i = \alpha^{R-\lfloor R/2\rfloor}(\alpha^k - \zeta_i)^S - \alpha^{-\lfloor R/2\rfloor}\eta_i(\alpha^k - (-b)^k\overline{\zeta_i})^S.$$

Note that

$$R \le |2m + (2n+k)v| \le 3\sqrt{X} = 9\sqrt{m}, \quad \text{and} \quad S = |v| \le \sqrt{X} = 3\sqrt{m}.$$

Let σ be an arbitrary element of $G = \mathrm{Gal}(K/\mathbb{Q})$. We then have that $\eta_i^\sigma = \eta_i'$, $\zeta_i^\sigma = \zeta_i'$, where η_i' and ζ_i' are roots of unity of order dividing s_1. Furthermore, $\alpha^\sigma \in \{\alpha, \beta\}$. If $\alpha^\sigma = \alpha$, we then get

$$\begin{aligned}
|G_i^\sigma| &= |\alpha^{R-\lfloor R/2\rfloor}(\alpha^k - \zeta_i')^S - \eta_i'\alpha^{-\lfloor R/2\rfloor}(\alpha - (-b)^k\overline{\zeta_i'})^S| \\
&\le \alpha^{(R+1)/2}(\alpha^k+1)^S + (\alpha^k+1)^S \\
&\le 2\alpha^{(R+1)/2}(\alpha+1)^{Sk} \le \alpha^{2+(9\sqrt{m}+1)/2+6\sqrt{m}k} \\
&\le \alpha^{11\sqrt{m}k},
\end{aligned} \tag{38}$$

while if $\alpha^\sigma = \beta$, we also get

$$\begin{aligned}
|G_i^\sigma| &= |\beta^{R-\lfloor R/2\rfloor}(\beta^k - \zeta_i')^b - \beta^{-\lfloor R/2\rfloor}\eta_i'(\beta^k - (-b)^k\overline{\zeta_i'})^S| \\
&\le (\alpha^{-k}+1)^S + \alpha^{R/2}(\alpha^{-k}+1)^S \\
&= \alpha^S + \alpha^{R/2+S} \le 2\alpha^{R/2+S} \le \alpha^{2+4.5\sqrt{m}+6\sqrt{m}} \\
&= \alpha^{11\sqrt{m}k}.
\end{aligned}$$

In the above, we used the fact that $\alpha^{-k}+1 \le \alpha^{-1}+1 \le \alpha$. In conclusion, inequality (38) holds for all $\sigma \in G$. Thus, if we write $G_i^{(1)}, \ldots, G_i^{(d)}$ for the d conjugates of G_i in K, we then get that

$$|\mathcal{N}_{K/\mathbb{Q}}(\mathcal{E}_i)| \le |\mathcal{N}_{K/\mathbb{Q}}(E_i)| = |\mathcal{N}_{K/\mathbb{Q}}(G_i)| \le \alpha^{11dk\sqrt{m}},$$

where the first inequality above follows because $\mathcal{E}_i$ divides E_i; hence G_i, and $E_i \neq 0$. Multiplying the above inequalities for $i = 1, \ldots, \ell$, we get that

$$\begin{aligned}
E^\ell = |\mathcal{N}_{K/\mathbb{Q}}(E)| = |\mathcal{N}_{K/\mathbb{Q}}(E\mathcal{O}_K)| &\le \left|\mathcal{N}_{\mathbb{K}/\mathbb{Q}}\left(\prod_{i=1}^{\ell}\mathcal{E}_i\right)\right| \\
&\le \left|\prod_{i=1}^{\ell}\mathcal{N}_{K/\mathbb{Q}}(G_i)\right| \le \alpha^{11d\ell k\sqrt{m}},
\end{aligned}$$

therefore

$$E \le \alpha^{11kd\sqrt{m}} \le \alpha^{22k\phi(s)\sqrt{m}} < \alpha^{22ks\sqrt{m}}. \tag{39}$$

In the above, we used that $d \le 2\phi(s) \le 2s$.

We are now ready to estimate A. We write

$$\begin{aligned}
A_1 &:= \gcd(U_m, U_{n+k}^2 - U_n^2);\\
A_2 &:= \gcd(U_m, U_{n+k}^2 + U_n^2);\\
A_3 &:= \gcd\left(U_m, \frac{U_{n+k}^6 - U_n^6}{U_{n+k}^2 - U_n^2}\right).
\end{aligned}$$

Clearly, $A \le A_1A_2A_3$. We bound each of A_1, A_2, A_3. We first estimate A_1 and A_2 and deal with A_3 later. Write

$$\begin{aligned}
U_n^2 &= \left(\frac{\alpha^n - \beta^n}{\alpha - \beta}\right)^2 = \frac{\alpha^{2n} + 2(-b)^n + \alpha^{-2n}}{(\alpha + b\alpha^{-1})^2};\\
U_{n+k}^2 &= \frac{\alpha^{2n+2k} + 2(-b)^n(-b)^k + \alpha^{-2n-2k}}{(\alpha + b\alpha^{-1})^2}.
\end{aligned}$$

Assume that $(-b)^k = 1$. If $\zeta \in \{\pm i\}$, then $(\alpha^k - (-b)^k\overline{\zeta})/(\alpha^k - \overline{\zeta}) = (\alpha^k + \zeta)/(\alpha^k - \zeta)$ is multiplicatively independent with α by Lemma 7. The argument which lead to inequality (39) shows that

$$A_2 \le \alpha^{11kd_1\sqrt{m}} \le \alpha^{44k\sqrt{m}}, \tag{40}$$

where $d_1 = 4$ is the degree of the field $\mathbb{Q}(\alpha, i)$. To estimate A_1, we set $\gamma = -b\alpha^2$ and, using that $(-b)^k = 1$, we find

$$\begin{aligned}
U_{n+k}^2 - U_n^2 &= \frac{\alpha^{2n+2k} + \alpha^{-2n-2k} - \alpha^{2n} - \alpha^{-2n}}{(\alpha + b\alpha^{-1})^2}\\
&= \alpha^{2-2n-k}\frac{(\gamma^{2n+k} - 1)(\gamma^k - 1)}{(\gamma - 1)^2},\\
U_m &= (-b\alpha)^{1-m}\left(\frac{\gamma^m - 1}{\gamma - 1}\right).
\end{aligned}$$

In the ring of integers $\mathcal{O} = \mathcal{O}_K$ of the quadratic field $K = \mathbb{Q}(\alpha)$ consider the ideals

$$\mathfrak{a} = \left(\frac{\gamma^m - 1}{\gamma - 1}, \frac{\gamma^{2n+k} - 1}{\gamma - 1}\right), \quad \mathfrak{b} = \left(\frac{\gamma^m - 1}{\gamma - 1}, \frac{\gamma^k - 1}{\gamma - 1}\right).$$

Clearly, $A_1 \mid \mathfrak{ab}$, whence

$$A_1^2 = \mathcal{N}_{K/\mathbb{Q}}(A_1) \leq |\mathcal{N}_{K/\mathbb{Q}}(\mathfrak{a})||\mathcal{N}_{K/\mathbb{Q}}(\mathfrak{b})|.$$

Clearly,

$$|\mathcal{N}_{K/\mathbb{Q}}(\mathfrak{b})| \leq \left|\mathcal{N}_{K/\mathbb{Q}}\left(\frac{(-b)^k\alpha^{2k}-1}{\alpha+b\alpha^{-1}}\right)\right| = |\mathcal{N}_{K/\mathbb{Q}}(U_k)| < \alpha^{2k}.$$

To estimate $|\mathcal{N}_{K/\mathbb{Q}}(\mathfrak{a})|$, observe that $\mathfrak{a} = (\gamma^d - 1)/(\gamma - 1)$ by item 3 of Corollary 5, where $d = \gcd(m, 2n + k)$. Using the obvious inequality $|\gamma^{-1}| \leq 1/2$, we get that

$$|\mathcal{N}_{\mathbb{K}/\mathbb{Q}}(\mathfrak{a})| = \left|\frac{\gamma^d-1}{\gamma-1}\frac{\gamma^{-d}-1}{\gamma^{-1}-1}\right| \leq 6|\gamma|^d = 6\alpha^{2d} < \alpha^{2d+4}.$$

Hence, $A_1 \leq \alpha^{d+k+2}$. It is important to note that $d \neq m$: otherwise we would have had $U_m \mid U_{n+k}^2 - U_n^2$, contradicting our hypothesis about the minimality of s. Therefore d is a proper divisor of m, showing that

$$A_1 \leq \alpha^{m/2+k+2}. \tag{41}$$

Thus, we have bounded A_1 and A_2 in the case $(-b)^k = 1$.

The case $(-b)^k = -1$ can be treated analogously, but A_1 and A_2 swap roles. This time for $\zeta \in \{\pm 1\}$ the number $\frac{\alpha^k-(-b)^k\overline{\zeta}}{\alpha^k-\zeta} = \frac{\alpha^k+\zeta}{\alpha^k-\zeta}$ is multiplicatively independent of α by Lemma 7, which implies the estimate

$$A_1 \leq \alpha^{22k\sqrt{m}}. \tag{42}$$

Next, using that $(-b)^k = -1$, we find

$$U_{n+k}^2 + U_n^2 = \alpha^{2-n-k}\frac{(\gamma^{2n+k}-1)(\gamma^k-1)}{(\gamma-1)^2},$$

and arguing exactly as in the case $(-b)^k = 1$, we get

$$A_2 \leq \alpha^{m/2+k+2}. \tag{43}$$

Hence, we get that both in case $(-b)^k = 1$ and in case $(-b)^k = -1$, we have

$$A_1A_2 \leq \alpha^{m/2+k+2+44k\sqrt{m}}. \tag{44}$$

Finally, for A_3, we note that by Lemma 7, unless $\alpha = 2 + \sqrt{3}$, we have that $\frac{\alpha^k-(-b)^k\overline{\zeta}}{\alpha^k-\zeta}$ is multiplicatively independent of α for $\zeta \in \{\pm\omega, \pm\omega^2\}$. Thus, writing

$$A_{3,\pm} = \gcd(A_3, U_{n+k}^2 \pm U_{n+k}U_n + U_n^2),$$

we get, by arguing in the field $\mathbb{Q}(\alpha, e^{2\pi i/3})$ of degree 4 as we did in order to prove inequality (39), that

$$A_{3,\pm} \leq \alpha^{44k\sqrt{m}}, \tag{45}$$

which leads to

$$A_3 \leq A_{3,+}A_{3,-} \leq \alpha^{88k\sqrt{m}}. \tag{46}$$

So, let us assume that $(a, b, k) = (4, 1, 1)$, so $\alpha = 2 + \sqrt{3}$. Note that since $U_t \equiv t \pmod 2$, it follows that $U_{n+k}^s - U_n^s = U_{n+1}^s - U_n^s$ is odd and a multiple of U_m, therefore m is odd. For $\zeta \in \{\omega, \omega^2\}$, we have that $\frac{\alpha^k - (-b)^k \overline{\zeta}}{\alpha^k - \zeta} = \frac{\alpha - \overline{\zeta}}{\alpha - \zeta}$ are multiplicatively independent of α, which leads, by the previous argument, to

$$A_{3,+} \leq \alpha^{44k\sqrt{m}}. \tag{47}$$

As for $A_{3,-}$, since

$$U_{n+1}^2 - U_{n+1}U_n + U_n^2 = V_{2n+1}/4,$$

we have that

$$A_{3,-} \mid \gcd(U_m, V_{2n+1}) = 1,$$

where the last equality follows easily from the fact that m is and $2n + 1$ are both odd (see (*iii*) of the Main Theorem in [3]). Together with (47), we infer that inequality (46) holds in this last case as well. Together with (44), we get that the inequality

$$A \leq A_1 A_2 A_3 \leq \alpha^{m/2+k+2+132k\sqrt{m}} \tag{48}$$

holds in all instances.

Inequality (28) together with estimates (29), (48) and (39), give

$$\alpha^{m-2} \leq U_m = DAE \leq \alpha^{6s+3+\log m/\log \alpha + m/2+k+2+(132k+22ks)\sqrt{m}}.$$

Since $s \geq 3$, we have $132 + 22s \leq 66s$. Since also $1/\log \alpha < 3$, we get

$$m/2 \leq (6s + 7 + 3\log m + k) + 66sk\sqrt{m}.$$

Since $m \geq 10000$, one checks that $6s + 7 + 3\log m + k < ks\sqrt{m}$. Hence,

$$m \leq 134ks\sqrt{m}, \tag{49}$$

which leads to the desired inequality (5).

4. Comment

One may wonder if one can strengthen our main result Theorem 1 in such a way as to include also the instances $s \in \{1, 2, 4\}$ maybe at the cost of eliminating finitely many exceptions in the pairs (a, k). The fact that this is not so follows from the formulae:

(i) $U_{n+k} - U_n = U_{n+k/2}V_{k/2}$ for all $n \geq 0$ when $b = 1$ and $2\|k$;
(ii) $U_{n+k} + U_n = U_{n+k/2}V_{k/2}$ for all $n \geq 0$ when $b = 1$ and $4 \mid k$ or when $b = -1$ and k is even;
(iii) $U_{n+k}^2 + U_n^2 = U_{2n+k}U_k$ for all $n \geq 0$ when $b = 1$ and k is odd,

which can be easily proved using the Binet formulas (6). Thus, taking $m = n + k/2$ (for k even) and $m = 2n + k$ for k odd and $b = 1$, we get that divisibility (3) always holds with some $s \in \{1, 2, 4\}$. We also note the "near-miss" $U_{4n+2} \mid 4(U_{n+1}^6 - U_n^6)$ for all $n \geq 0$ if $(a, b, k) = (4, -1, 1)$.

Acknowledgments

This work was done during a visit of T.K., A.P. and P.S. to the School of Mathematics of the Wits University in September 2015. They thank the School for hospitality and support and Kruger National Park for excellent working conditions. F.L. thanks Professor Igor Shparlinski for some useful suggestions. Yu.B. was partially supported by Max-Planck-Institut für Mathematik at Bonn. T.K. was partially supported by the Hubei provincial Expert Program in China. A.P. was partly financed by Project DIUV-REG N° 25-2013.

References

[1] Yu. Bilu, G. Hanrot, P.M. Voutier, Existence of primitive divisors of Lucas and Lehmer numbers, with an appendix by M. Mignotte, J. Reine Angew. Math. 539 (2001) 75–122.
[2] T. Komatsu, F. Luca, Y. Tachiya, On the multiplicative order of F_{n+1}/F_n modulo F_m, in: Proc. of the Integers Conference 2011, Integers B 12 (2012/2013) A8.
[3] W.L. McDaniel, The G.C.D. in Lucas sequences and Lehmer number sequences, Fibonacci Quart. 29 (1991) 24–29.